DMDC's Role in Identity Protection and Management

Worldwide Leadership in Identity

Prepared for:
Biometric Symposium

March 18, 2004

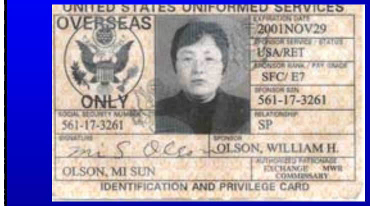
Presented by:
Kenneth C. Scheflen

What is Personnel Identity Protection?

- Establishment of identity is a basic business function - who are my employees, customers, suppliers
- In the past this was taken for granted - people were who they said they claimed to be
- Today assumptions about identity can create security issues
- Each business or government must take steps to provide assurance of identity - foundation of sound business practice

Why Personnel Identity Protection is Important???

Counterfeit Credentials are Common

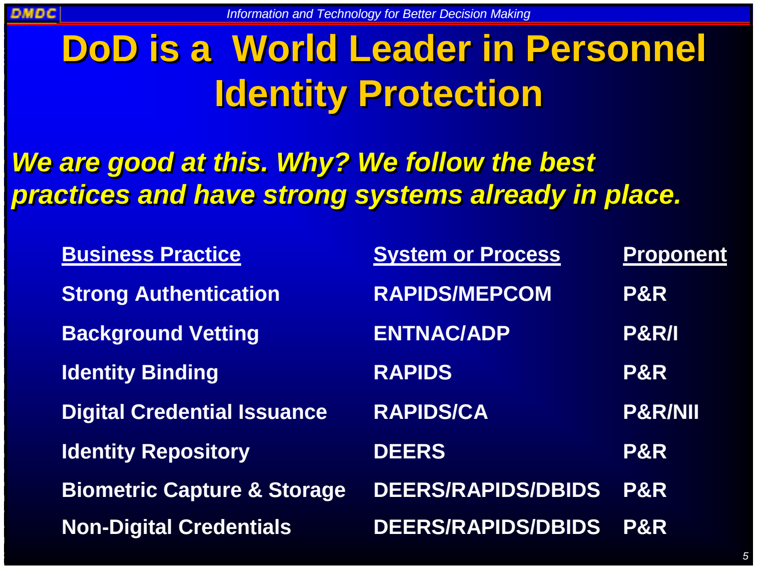


Courtesy USFK Provost Marshall

- Fakes come as a package – with everything needed
- Overseas hundreds of fakes are detected
- For physical security – authenticating the ID is rare

Personnel Identity Protection is a Process

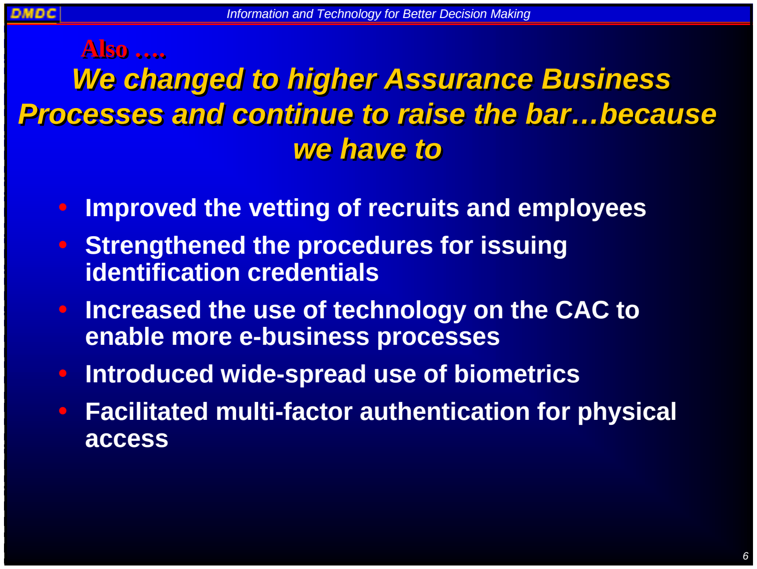
1. Strong authentication of the individual
   - A face to face interaction between the individual and a trusted agent
   - A business process that provides sufficient evidence of identity -- checks of public records, background investigations, examination of primary documents
2. Binding the identity to a management system
   - A credential is the best linkage to the personnel identity protection system
3. Binding the credential to the individual
   - Biometrics and PINs bind the credential to the person
   - Credential then becomes a proxy for digital/physical access given technology is used
4. Authentication of the credential at all access points
   - Logical and Physical
5. Safeguarding identity information from unwarranted disclosure



DoD is a World Leader in Personnel Identity Protection

We are good at this. Why? We follow the best practices and have strong systems already in place.

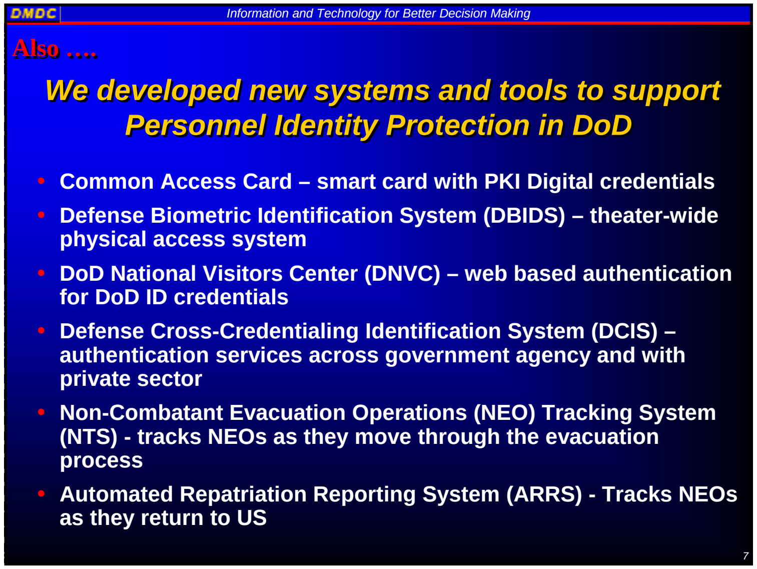
Business Practice	System or Process	Proponent
Strong Authentication	RAPIDS/MEPCOM	P&R
Background Vetting	ENTNAC/ADP	P&R/I
Identity Binding	RAPIDS	P&R
Digital Credential Issuance	RAPIDS/CA	P&R/NII
Identity Repository	DEERS	P&R
Biometric Capture & Storage	DEERS/RAPIDS/DBIDS	P&R
Non-Digital Credentials	DEERS/RAPIDS/DBIDS	P&R



Also ….

We changed to higher Assurance Business Processes and continue to raise the bar…because we have to

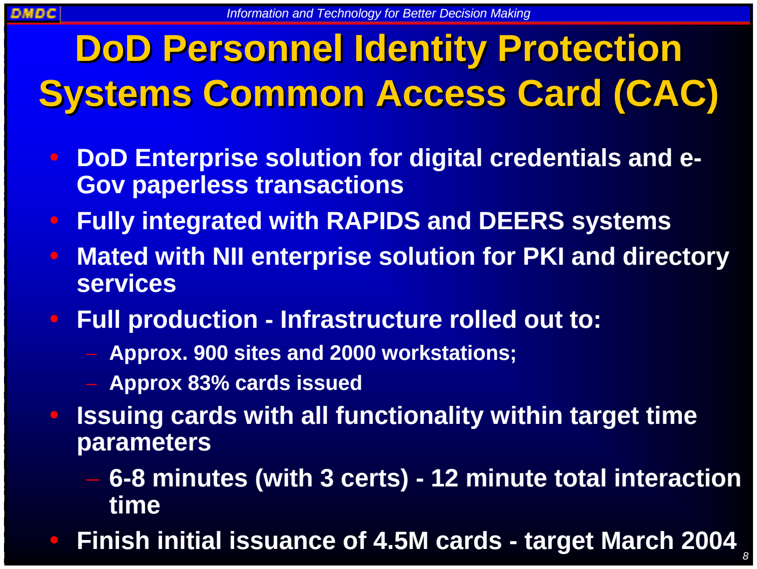
- Improved the vetting of recruits and employees
- Strengthened the procedures for issuing identification credentials
- Increased the use of technology on the CAC to enable more e-business processes
- Introduced wide-spread use of biometrics
- Facilitated multi-factor authentication for physical access



Also ….

We developed new systems and tools to support Personnel Identity Protection in DoD

- Common Access Card – smart card with PKI Digital credentials
- Defense Biometric Identification System (DBIDS) – theater-wide physical access system
- DoD National Visitors Center (DNVC) – web based authentication for DoD ID credentials
- Defense Cross-Credentialing Identification System (DCIS) – authentication services across government agency and with private sector
- Non-Combatant Evacuation Operations (NEO) Tracking System (NTS) - tracks NEOs as they move through the evacuation process
- Automated Repatriation Reporting System (ARRS) - Tracks NEOs as they return to US



DoD Personnel Identity Protection Systems Common Access Card (CAC)

- DoD Enterprise solution for digital credentials and e-Gov paperless transactions
- Fully integrated with RAPIDS and DEERS systems
- Mated with NII enterprise solution for PKI and directory services
- Full production - Infrastructure rolled out to:
  - Approx. 900 sites and 2000 workstations;
  - Approx 83% cards issued
- Issuing cards with all functionality within target time parameters
  - 6-8 minutes (with 3 certs) - 12 minute total interaction time
- Finish initial issuance of 4.5M cards - target March 2004

DoD Personnel Identity Protection Systems Defense Biometric Identification System (DBIDS)

DBIDS is a personnel identity protection and force protection system that:

- Uses existing DoD issued identification credentials
- Is scalable to cover a building, an installation, or an entire theater of operations
- Contains information on the individual, a digital photo, and a digital fingerprint
- Allows level of authentication to vary by threat level or at local commander's option
- Is rule driven - configurable by local authorities to meet their business rules for access
- Issues badges for individuals not authorized DoD credentials under DoD Instruction 1000.13
- Largest Physical Access System in DoD and largest use of biometrics for access in the Department

DBIDS

Germany

Korea

- Korea – fully deployed 250K registrations
- Japan – planning on-going
- Europe – Registration over 175K+ - gates now operational
- Kuwait – system deployed - registration underway

Kuwait

DoD Personnel Identity Protection Systems

DoD National Visitors Center (DNVC)	DoD Cross-Credentialing Identification System (DCIS)
Authenticates DoD ID Credential holders at DoD bases and facilities for physical access	**Authenticates** Federated Commercial and Government ID Credentials at each others' facilities

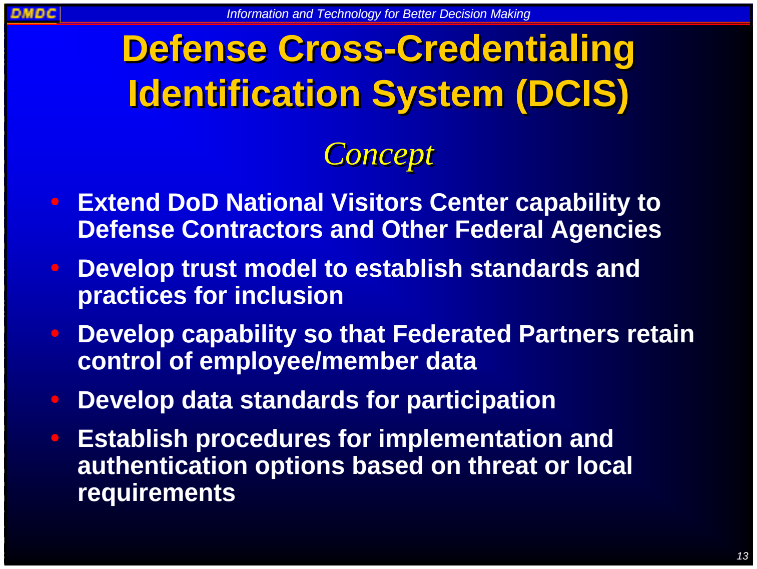
Features:

- Secure Web-based access within DoD and between Partners
- Signed delivery of authentication data including biometrics
- Trust server can be scaled to add federated partners quickly
- Standards based using signed XML

DoD National Visitors Center (DNVC)

Concept

- Authentication of DoD Credentials increasing requirement
- Services need web based, enterprise-wide capability – anywhere, any credential requiring only a browser
- Use comprehensive DEERS/RAPIDS data store to provide information
- Incorporate biometrics – photo and fingerprint (fingerprint matching an option – requires reader and client software)
- Accommodates Members, retirees and families
- Links strong authentication to base access systems and local access policies

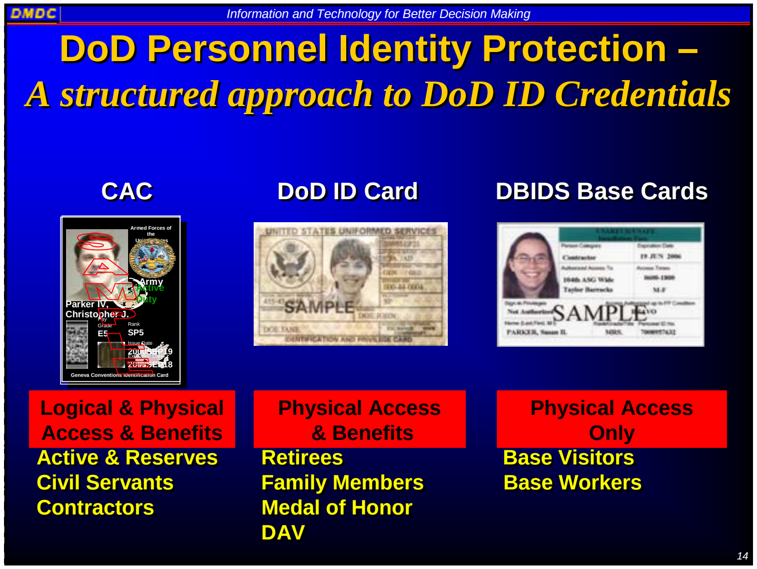


DMDC | Information and Technology for Better Decision Making

Defense Cross-Credentialing Identification System (DCIS)

Concept

- Extend DoD National Visitors Center capability to Defense Contractors and Other Federal Agencies
- Develop trust model to establish standards and practices for inclusion
- Develop capability so that Federated Partners retain control of employee/member data
- Develop data standards for participation
- Establish procedures for implementation and authentication options based on threat or local requirements

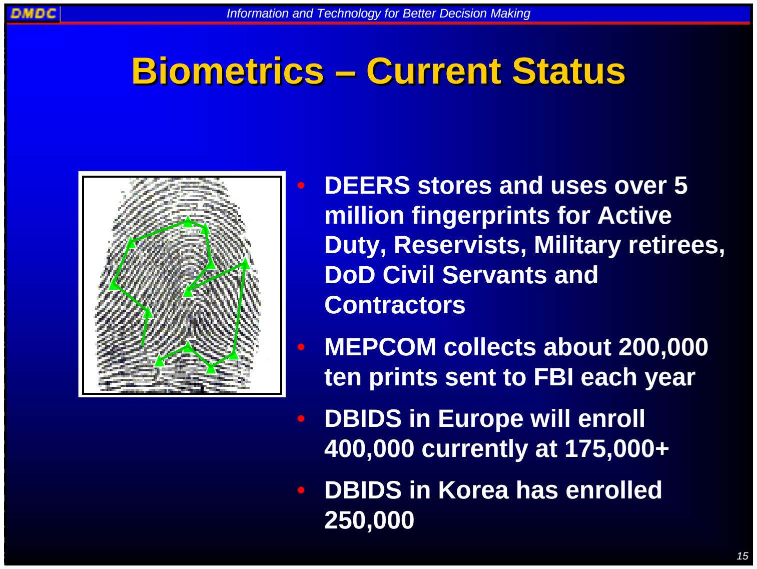


DMDC | Information and Technology for Better Decision Making

DoD Personnel Identity Protection – *A structured approach to DoD ID Credentials*

CAC	DoD ID Card	DBIDS Base Cards
Logical & Physical Access & Benefits	Physical Access & Benefits	Physical Access Only
Active & Reserves Civil Servants Contractors	Retirees Family Members Medal of Honor DAV	Base Visitors Base Workers

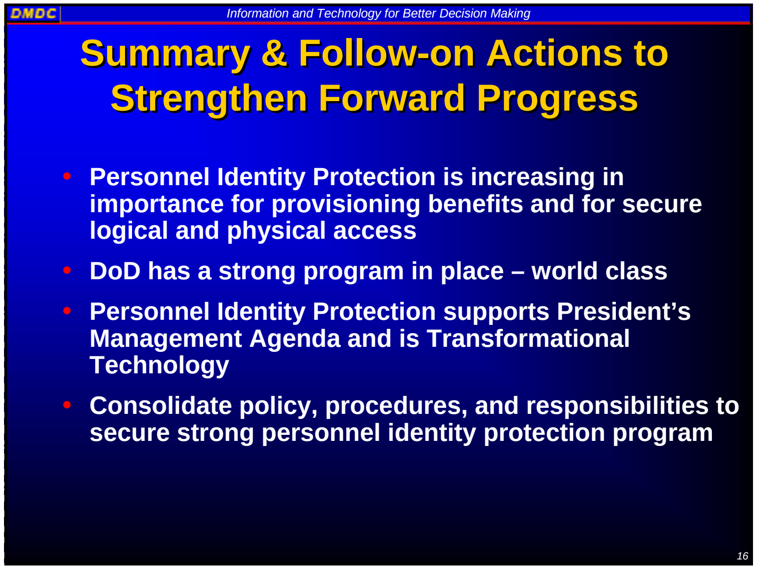
Armed Forces of the United States
Parker IV, Christopher J.
Army
E5
SP5
Geneva Conventions Identification Card
UNITED STATES UNIFORMED SERVICES
SAMPLE
IDENTIFICATION AND PRIVILEGE CARD
SAMPLE



DMDC | Information and Technology for Better Decision Making

Biometrics – Current Status

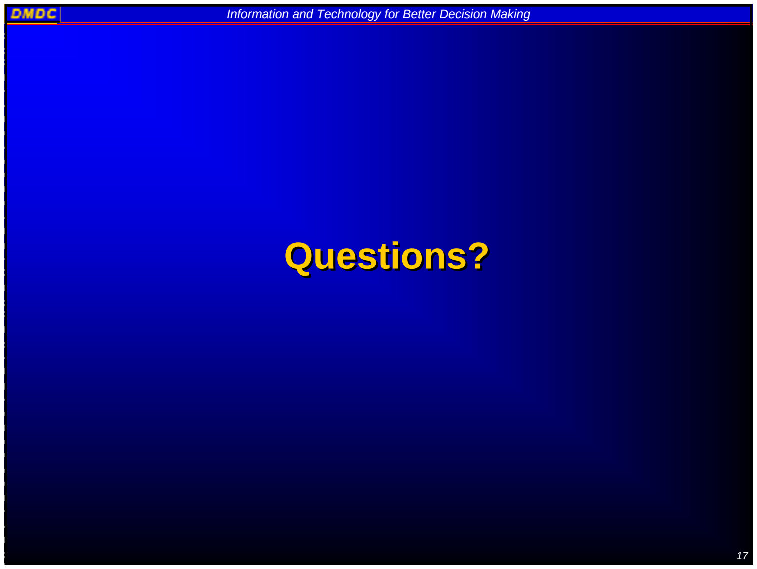
- DEERS stores and uses over 5 million fingerprints for Active Duty, Reservists, Military retirees, DoD Civil Servants and Contractors
- MEPCOM collects about 200,000 ten prints sent to FBI each year
- DBIDS in Europe will enroll 400,000 currently at 175,000+
- DBIDS in Korea has enrolled 250,000



DMDC | Information and Technology for Better Decision Making

Summary & Follow-on Actions to Strengthen Forward Progress

- Personnel Identity Protection is increasing in importance for provisioning benefits and for secure logical and physical access
- DoD has a strong program in place – world class
- Personnel Identity Protection supports President's Management Agenda and is Transformational Technology
- Consolidate policy, procedures, and responsibilities to secure strong personnel identity protection program



DMDC Information and Technology for Better Decision Making

Questions?

17